Heather Lopez (SBN 354022)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: hlopez@milberg.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
Yuanchen Lu (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PETER C. HAYWARD, individually and on behalf of all others similarly situated, Plaintiff, v. MPARTICLE, INC., and ROKT US CORP., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Peter C. Hayward, individually and on behalf of all other similar situated individuals, asserts the following against Defendant mParticle, Inc. and Rokt US Corp. (collectively, "mParticle") based upon personal knowledge, information and belief (where applicable), and the investigation of counsel. The Court has jurisdiction over these claims as stated in Paragraphs 42 through 60.

SUMMARY OF ALLEGATIONS

1.   Few, if any, consumers have heard the name "mParticle." But mParticle knows their names. It also knows their email, phone number, unique devices, and exactly what they are doing across the internet, so long as mParticle's inconspicuous tracking technology is running in the background. mParticle stores all this information in a consolidated and enriched user profile.

2.   mParticle obtains consumers' identifying information through its product "IDSync" which it launched in 2017. Through this identity "solution"—and complimentary products (e.g., its SDK and other tracking technology)—mParticle has been secretly harvesting and monetizing directly identifiable user data from millions of U.S. residents without their knowledge.

3.   IDSync operates by assigning an mParticle ID to individual users of all websites and apps that incorporate the mParticle software. The mParticle ID serves as the anchor for the entirety of the user's mParticle profile. mParticle ID boasts its technology is on hundreds of thousands of websites.

4.   Whenever an individual visits a website or app that uses mParticle, its IDSync software attempts to identify the user in as many ways as it can, for instance, by intercepting full name, email, phone number, and any other identifiers mParticle can get its hands on. Each time mParticle intercepts a piece of identifying information, it adds it to the user's existing identity profile and associates it with that user's mParticle ID. Through this data collection process, mParticle has created an entire directory full of personally identifiable information on millions of U.S. residents.

CLASS ACTION COMPLAINT – CASE NO. _____

5.   Through the mParticle SDK and other tracking technology, mParticle also intercepts users' searches, queries, and other activity on websites and apps. In many instances, mParticle's tracking technology can be found on websites and apps that involve inherently private information, including websites used to make financial transactions or apps used to privately watch videos. This data is stored alongside the identifying information mParticle collects about each user in the same user profile.

6.   Because mParticle does not rely exclusively on cookies, it circumvents traditional privacy-preserving mechanisms. For instance, traditional third-party cookies can be blocked, expire after a limited period of time, and can be reset. Users can also avoid cookies by using privacy-preserving browsers, like Mozilla Firefox. mParticle bypasses cookie blockers, privacy-preserving browsers, and incognito mode—leaving consumers at the mercy of mParticle's collection of their data.

7.   Worse, one of mParticle's primary selling points to customers is its integrations with dozens of the largest advertising companies in the world. mParticle forwards its detailed customer profiles to these ad networks so that individual users can be targeted with ads based on their mParticle profiles.

8.   mParticle charges customers for every part of this process, from data collection and processing to storage and integrations through what it calls "value-based pricing."[1] Its customer profiling is so popular that mParticle was recently acquired for over $300 million.

9.   Plaintiff and Class Members had no knowledge that mParticle was using unique identifiers to track them across the web, mobile applications, and other internet-connected devices, or that it was using this data to create comprehensive user profiles and facilitate highly-specific targeted advertising.

---

[1] *Pricing: One Platform, One Rate, Zero Restrictions*, MPARTICLE, https://www.mparticle.com/pricing/ (last visited Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

10.   mParticle offers no consumer facing policies or disclosure at the time it intercepts Plaintiff and Class Members' data, nor does it prompt users viewing the websites or other web properties of its presence.

11.   mParticle's interception of the contents of Plaintiff's and Class Members' communications with third parties through its tracking technology violates Cal. Penal Code § 631 and § 632, and its installation of a tracking device on each of the websites used across the internet violates Cal. Penal Code § 638.51(a), as well as other laws.

PARTIES

A. Plaintiff

12.   Plaintiff **Peter Hayward** is a resident of Los Angeles County, California.

13.   Plaintiff Hayward used several online services, including Venmo, JetBlue, and Peacock, that implemented mParticle's IDSync and other tracking technology.

14.   Unbeknownst to Plaintiff Hayward, mParticle assigned Plaintiff Hayward mParticle IDs ("mpid").

15.   When Plaintiff Hayward logged in to these services, mParticle searched for and collected his directly identifiable information.

16.   For instance, when Plaintiff Hayward used the **Peacock** app, mParticle intercepted his email address. It also collected the mParticle ID, a User ID assigned by Peacock, and Plaintiff Hayward's advertising ID ("IDFA"), which is a persistent device identifier.

17.   mParticle also obtains an mParticle device ID ("mp_deviceid"), which is a separate unique ID for the device he used to sign-in to Peacock at that time. If Plaintiff Hayward ever logged in with a different device, that device receives its own separate unique ID that is added to Plaintiff Hayward's user profile.

18.   mParticle also intercepted Video Title IDs and Video IDs while Plaintiff Hayward used the Peacock service, which reveals the precise video content viewed by Plaintiff Hayward.

CLASS ACTION COMPLAINT – CASE NO. _____

19.   mParticle processed and enriched all the data it intercepted from Plaintiff Hayward's communications with Peacock and stored this information in a consolidated user profile.

20.   When Plaintiff Hayward logged on to Venmo website,[2] mParticle also intercepted directly identifiable information, including his email address, Venmo name (typically, first-last), and phone number. It also collected the mParticle ID, mParticle device ID, and a unique customer ID set by Venmo.

21.   When Plaintiff Hayward made transactions on the **Venmo** website, mParticle intercepted the details of these transactions. Specifically, mParticle intercepted: (1) that Plaintiff Hayward was making a payment; (2) the recipient name; (3) recipient username; (4) that the profile type was "personal"; (5) the exact amount of the transaction; and (6) the "note" that accompanies the payment describing what the payment is for. This information is sent even if the user marked their profile as private, *i.e.*, chose that their transactions should not be seen my anyone else other than the recipient.

22.   mParticle processed and enriched all the data it intercepted from Plaintiff Hayward's communications with Venmo and stored this information in a consolidated user profile.

23.   The information described above is transmitted regardless of whether Plaintiff Hayward declined cookies and regardless of whether he used private browsing mode or selected "Do Not Track" on their mobile device.[3] In short, Plaintiff Hayward had no way to "block" mParticle's hidden tracking tools from surreptitiously collecting his data, including his personally identifiable information.

24.   Plaintiff Hayward did not consent to mParticle intercepting his personally identifiable information, assigning and using unique identifiers to track him across internet-enabled services and devices, or intercepting and using the contents of his private communications for mParticle's and others' profit.

---

[2] The Venmo app similarly incorporated mParticle's IDSync and other tracking technologies.

[3] Using "Do Not Track" would only prevent the interception of IDFA, not the directly identifiable information mParticle collects about the user.

CLASS ACTION COMPLAINT – CASE NO. _____

B. Defendant

25.   **mParticle, Inc.**[4] is a Delaware corporation with its principal place of business located in New York, New York.

26.   mParticle knowingly and intentionally developed IDSync to track Plaintiff and Class Members across internet-connected services and build comprehensive user-specific profiles.

27.   mParticle knew that its IDSync software, including mParticle ID, circumvented existing privacy protections (such as "Do Not Track" and widespread adoption of third-party cookie blocking by major browsers like Safari and Firefox) because it developed this identifier specifically as an alternative to such privacy-preserving mechanisms.

28.   mParticle offered these services to websites, mobile applications, and other customers so it would have a unique way of tracking Plaintiff and Class Members across devices and platforms that it could monetize for profit.

29.   mParticle knowingly and intentionally used its IDSync tracking tool, and related tracking technology, to develop comprehensive user profiles and charge mParticle's customers to access and integrate these profiles into their advertising.

30.   mParticle knew that this data was sent to advertising companies because it provided documentation and easy-to-use methods for its customers to activate this data with ad providers. mParticle directly sent this data to ad providers through data forwarding.

31.   mParticle marketed its technology as offering "privacy-preserving" identity resolution, despite understanding it created a software capable of tracking users at the individual level in a manner tied to permanent, directly identifiable information, like email and phone number.

32.   **Rokt US Corp.** is a Delaware corporation with its principal place of business located in New York, New York.

---

[4] "mParticle" as used in this section refers solely to mParticle, Inc.

6

33.   Rokt is an e-commerce marketing platform that specializes in offering targeted advertisements on online customer check-out pages. Rokt monetizes the check-out confirmation page by showing targeted advertisements from brands that the consumer is likely to engage with.

34.   Rokt is used by over 30,000 ecommerce brands.

35.   Rokt makes money from publishers (i.e., the websites and apps that show the advertisement) and advertisers (i.e., the companies whose advertisement is shown to the consumer). For publishers to use Rokt, they integrate its SDK or API on their existing websites.

36.   Rokt relies on AI and machine learning to determine which advertisements to show individual consumers based on behavioral, demographic, and other data. Rokt uniquely identifies each individual user that will see Rokt-powered ads through both deterministic and contextual data, including names, email addresses (both raw and hashed), and other identifiers.

37.   Since 2018, Rokt has acknowledged that the "cookie-based framework" relied on by advertisers is "fundamentally incapable of driving truly person-based marketing activity" for the reasons described herein.[5]

38.   It actively advocated for identity graphs—like those used by mParticle—to track users without relying on cookies, including by stitching email addresses and other personally identifiable information in a unique "persistent ID profile."[6]

39.   Rokt merged with mParticle in January 2025. mParticle provides the precise identity graph Rokt found imperative to power advertising software and engage in user-specific ad targeting.

40.   As put by Rokt's CEO and co-founder, Bruce Bechanan, combining the two companies will enable them "to bring [a] significant performance lift to [both] of [their]

---

[5] Alex Edholm & Vladi Kuschnerov, *Moving from Cookies to Persistent Identity: A Meatier Solution to User Data*, ROKT (Sept. 17, 2018), https://www.rokt.com/blog/moving-cookies-persistent-identity-user-data/ (last visited Apr. 22, 2025).
[6] *Id.*

CLASS ACTION COMPLAINT – CASE NO. _____

clients."[7] Rokt customers will be able to access mParticle's "real-time customer data platform"[8]—powered by IDSync—to ensure their advertisements are "truly person-based"[9] and mParticle customers will be able to immediately integrate the mParticle enhanced user profiles with Rokt advertising.

41.   Rokt knew that mParticle's identity software thwarted existing privacy protections. Rokt was well aware that the decline of cookies prevented person-level ad targeting and was actively advocating for an identity graph like the one offered by mParticle. Its merger with mParticle was intentional, precisely so it could use this feature in its own business model.

JURISDICTION AND VENUE

42.   Jurisdiction is proper under 28 U.S.C § 1332(d) because: (1) the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, (2) there are more than 100 putative members of the Class, and (3) a significant portion of Class Members are citizens of a state different from mParticle.

43.   **mParticle.** This Court has personal jurisdiction over mParticle because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State, including the interception, use, and storage of Plaintiff Hayward's and other California residents' personally identifiable information and other private data. mParticle engages in these activities for profit.

44.   mParticle knew Plaintiff Hayward and other California residents resided in California when it intercepted and stored their data because mParticle: (1) knew the identity of each individual whose data it intercepted through its IDSync technology; and (2) received IP addresses and geolocation information, which further reveals their precise location.

---

[7] *Rokt And Mparticle Merge To Redefine Real-Time Relevance*, MPARTICLE, https://www.mparticle.com/news/rokt-and-mparticle-merge/ (last visited Apr. 22, 2025).
[8] *Id.*
[9] Alex Edholm & Vladi Kuschnerov, *Moving from Cookies to Persistent Identity: A Meatier Solution to User Data*, ROKT (Sept. 17, 2018), https://www.rokt.com/blog/moving-cookies-persistent-identity-user-data/ (last visited Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

45.   mParticle purposefully availed itself of this forum by, among other things, marketing and selling its IDSync and other tracking technology to California companies and companies who offer apps and websites in California.

46.   mParticle advertises on its website that its customers include SoFi—based in San Francisco—and include a SoFi client testimonial describing how mParticle has made it "easier" for SoFi to "create a 360-degree view of the customer" and use mParticle's enhanced "data to improve targeting and personalization[.]"[10] mParticle's other California-based customers include Airbnb, Postmates, Drybar, and PayPal, among others.[11]

47.   mParticle actively sought out other benefits from this State, including partnering with California companies to whom it forwards and shares Plaintiff's and Class members' data. mParticle has strategic partnerships with numerous California-based companies including Meta, Google, LiveRamp, and Adobe.[12] mParticle customer data platform, powered by IDSync, integrates with these companies' ad platforms specifically for re-targeting (i.e., so Plaintiff and Class Members can be targeted with ads) and to combine analytics (i.e., the data each respective company has about the user).

48.   mParticle maintains an office in San Francisco, California. mParticle's current and former employees, including executive officers, are based in California. For instance, mParticle's former Chief Marketing Officer, Jason Seeba, was based in the San Francisco Bay Area,[13] as was its former Head of Data, Patrick Tangphao.[14] A current Senior Manager of Strategic Accounts, Nicholas Craig, is also based in the San Francisco Bay Area.[15]

---

[10] *Trusted By Data-Driven Teams Worldwide*, MPARTICLE, https://www.mparticle.com/customers/ (last visited Apr. 22, 2025).

[11] *mParticle: Company Overview,* CHIEFDISRUPTOR, https://www.chiefdisruptor.com/mparticle (last visited Apr. 22, 2025).

[12] *Connect Your Data Anywhere*, MPARTICLE, https://www.mparticle.com/integrations/ (last visited Apr. 22, 2025).

[13] Jason Seeba, LINKEDIN, https://www.linkedin.com/in/jasonseeba/ (last visited April 22, 2025).

[14] Patrick Tangpaho, LINKEDIN, https://www.linkedin.com/in/patricktangphao/ (last visited April 22, 2025).

[15] Nicholas Craig, LINKEDIN, https://www.linkedin.com/in/nicholaslcraig/ (last visited April 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

mParticle's LinkedIn list 26 employees in California,[16] with 17 of those in the San Francisco area, out of just 144 U.S. employees.[17] Thus, nearly 20% of mParticle's workforce is based in this State.[18]

49.   In addition to profiting from the sale of its IDSync product and tracking technology in California, as well as hosting and using California user data for profit, mParticle further targets the California market by attending and participating in marketing events in the forum.

50.   For instance, mParticle's CEO and Co-Founder, Michael Katz, attended and participated in the Activate Summit in September 2022 in San Francisco.[19] mParticle's CEO gave a presentation titled "The Complexity of Customer Identity and Its Role in Personalization."[20] This presentation specifically discussed the changing "privacy landscape" (described herein),[21] and how companies can transform "unknown users" into "known users" by using mParticle's software.[22] This presentation was co-hosted by Hidekazu Ii, Senior Director of Product, Consumer Identity at NBCUniversal—an mParticle client. Mr. Ii described how NBC gets "every single piece of data" into mParticle across its digital properties, including data reflecting their email addresses, their first and last name, date of birth, and "where they live."[23]

51.   Similarly, mParticle's Director of Product and Sales Engineering and a Senior Solutions Engineer attended App Growth Masterminds SF in April 2022 in San Francisco, California. They co-led a presentation called "It's Chaos! How to Overcome Customer Data Headaches and Develop a Winning First-Party Data Strategy." This presentation

---

[16] mParticle by Rokt, PEOPLE | LINKEDIN, https://www.linkedin.com/company/mparticle-inc-/people/ (last visited April 22, 2025).
[17] *Id.*
[18] *Id.*
[19] *Activate Summit*, ITERABLE, https://activate.iterable.com/noam/2022-recordings/ (last visited Apr. 22, 2025).
[20] *Id.*
[21] *The Complexity of Customer Identity and Its Role in Personalization*, ITERABLE, https://activate.iterable.com/schedule/noam/2022/tech-stack-deep-dive/ (last visited Apr. 22, 2025).
[22] *Id*.
[23] *Id*.

CLASS ACTION COMPLAINT – CASE NO. _____

similarly centered around how the "introduction of privacy regulations" has led to "chaos" and how "brands" can use mParticle to "deliver[] winning customer experiences."[24]

52.   Upon information and belief, mParticle generates substantial revenue through its California operations, including its provision and sale of its IDSync product and tracking technology to California companies and its hosting of California users' data for profit.

53.   **Rokt**. This Court has personal jurisdiction over Rokt because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in this State, including the use of California residents' personally identifiable information and other private data for targeted advertising. Rokt engages in these activities for profit.

54.   Rokt knew it used California residents' data in connection with its advertising services because: (1) it has and uses the mParticle customer data platform, which includes data revealing the identity of each individual user, including their location; (2) it receives data from advertisers and publishers, further revealing users' identities.

55.   Rokt purposefully availed itself of this forum by, among other things, marketing and selling its targeted advertising product to California companies and companies who offer apps and websites in California. This includes Lyft, Uber, and Hulu[25]—all headquartered in California. Uber specifically is listed as using Rokt to "[u]nlock additional profitability in the checkout flow."[26]

56.   Rokt actively sought out other benefits from this State, including partnering with California companies. One of Rokt's ecommerce partners with whom it integrates its technology is Salesforce—based in California. Its technology partners also include California companies, including Adobe and LiveRamp.[27]

---

[24] *App Growth Masterminds San Francisco*, AGS APP GROWTH SUMMIT, https://appgrowthsummit.com/events/app-growth-masterminds-sf-2022/ (last visited Apr. 22, 2025).
[25] *Rokt*, CBINSIGHTS, https://www.cbinsights.com/company/rokt/customers? (last visited Apr. 22, 2025).
[26] *Id.*
[27] *Partner With Rokt*, ROKT, https://www.rokt.com/partners/ (last visited Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

57.   Rokt maintains an office in San Francisco, California.[28] Importantly, Rokt's Co-Founder and former Chief Innovation Officer and board member, Justin Viles, is based in California.[29]

58.   Upon information and belief, Rokt generates substantial revenue through its California operations, including its provision and sale of its advertising product to California companies and its use of California users' data for profit.

59.   Venue is proper under 28 U.S.C. §1391(b), (c), and (d) because a substantial portion of the conduct described in this Class Action Complaint was carried out in this District. mParticle maintains substantial business operations in this District, including, upon information and belief, activities implementing mParticle's IDSync, managing data partnerships, and facilitating targeted advertising through integration with California advertising platforms.

60.   Pursuant to Civil L.R. 3-2(c), the assignment to the division is proper because a substantial part of the conduct which gives rise to Plaintiff's claims occurred in this District. mParticle's conduct, as described herein, is directed at Internet users and people throughout the United States, including in San Francisco County, California, where mParticle maintains offices and business operations.

BACKGROUND OF USER TRACKING

61.   Over a decade ago, Apple, Inc. announced that it would no longer allow app developers to intercept "UDIDs" which are unique, device-specific identifiers. These persistent identifiers were deprecated because they are seen as privacy intrusive—they cannot be reset and were used to facilitate device-specific targeted advertising.

62.   Starting in 2020, Apple, Inc. and Google, LLC rocked the digital advertising world once again by announcing the eventual deprecation of advertising identifiers (IDFA and ADID) and third-party cookies in favor of more privacy-preserving mechanisms. Advertising identifiers were seen as a replacement for UDIDs because they could be reset

---

[28] *We Are Rokt*, ROKT, https://www.rokt.com/about-us/ (last visited Apr. 22, 2025).
[29]   Justin Viles, LINKEDIN, https://www.linkedin.com/in/justinviles (last visited April 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

by the user, as can third-party cookies. However, this did not change the fact that they are ultimately privacy-invasive, as they allow ad targeting at the user level.

63.   This created serious concerns within the multi-billion-dollar digital advertising industry. Digital advertisers relied on these device identifiers and cookies to uniquely identify individuals who use their products and services—and other entities' products and services—to curate and serve targeted advertisements to individuals, based on profiles of information reflecting web and app activity indexed to unique identifiers present in third-party cookies.

64.   For instance, a mobile app developer would use identifiers like the IDFA and ADID created by iOS and Android phones to track user activity across their mobile application, understand what actions users took, and their preferences, interests, and other information. The company would then send that information to an advertising company, such as Google, to serve targeted advertisements to that customer using this unique identifier.

65.   While companies scrambled to find solutions to the eventual deprecation of unique device identifiers and third-party cookies, many of those options were not nearly as lucrative. For instance, many companies began tracking "sessions" (i.e., one interaction with the webpage) and then sought to use cross-device tracking alternatives to match each of these unique sessions to the same user. However, this alternative is not nearly as powerful as directly tracking an individual at the *user*-level rather than *session*-level.

MPARTICLE'S UNIQUE IDENTIFIERS

66.   mParticle capitalized on the move away from device identifiers and third-party cookies by creating a persistent, unique, cross-platform identifier *of its own* designed precisely to "[u]nify real-time customer interactions" for better "personalization, more complete customer journey insights, and better machine learning."[30]

67.   mParticle's identity software is called IDSync. IDSync is used to profile and

---

[30] *Customer 360*, MPARTICLE, https://www.mparticle.com/platform/customer-360/ (last visited Apr. 11, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

identify individual users, every one of their separate devices, and their actions and behaviors. IDSync accomplishes this by collecting "[e]very piece of data" about a user, and "stor[ing]" this data "in a user profile."[31] mParticle *itself* describes this process as occurring "[b]ehind the scenes"[32]—*i.e.*, hidden from the user's view.

68.   Whenever a user opens a website or app that uses the mParticle software, an identity request is automatically made to mParticle. To identify users, mParticle uses three steps. First, "[a]n identification request" is made through "one of the mParticle platform SDKs or the HTTP API" through which mParticle intercepts an end user's identifying information such as email, customer IDs, or device identifiers or other information that can be used to identify and track the user. Next, "mParticle looks for a matching user profile" by "comparing the identifiers included in the request with" identifiers already in mParticle's system. Finally, mParticle returns a matching user profile to the client if it finds a match.[33]

69.   mParticle performs this process at the beginning of an app or website session, at login, and at logging out. If mParticle identifies any additional identifying information about the user during the app or website session (such as the user entering an email address or phone number during the session), mParticle intercepts that identifying piece of information and adds it to that user's existing user profile.

70.   If there is no match, mParticle creates a new user profile and assigns a new unique mParticle ID for the purpose of future identification. mParticle adds identifying information to the user profile as it identifies it on the website or app used by the user.

71.   The mParticle ID is an important building block of mParticle's identity tracker. It is "a 64-bit signed integer that is used by mParticle to uniquely identity a user

[31] *Identify Users*, MPARTICLE, https://docs.mparticle.com/guides/idsync/identify-users/ (last visited Apr. 22, 2025).

[32] *Store and Organize User Data*, MPARTICLE, https://docs.mparticle.com/guides/idsync/user-data/ (last visited Apr. 22, 2025)

[33] *Identify Users*, MPARTICLE, https://docs.mparticle.com/guides/idsync/identify-users/ (last visited Apr. 11, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

for the purposes of processing User Identities and Profile data."[34] "All users" are "assigned an [mParticle] ID for the purposes of retrieving profile data" when their data is sent to mParticle.[35] Thus, the mParticle ID serves as the anchor for the user's identity profile.

72.   As Figure 1 shows, an mParticle client can simply type in the mParticle ID—or any other known identifier like email address, customer ID, or device ID—in a search box to pull all the profile data mParticle linked to that specific user.

FIGURE 1

User Search

| -2032428432473887573 | mParticle ID ⌄ | 🔍 Search |

You may search by User ID, Name, or any other Field

73.   Once any of these identifiers are entered, mParticle returns the user's specific profile, as shown in Figure 1.

74.   As shown below, the user profile contains the mParticle ID, as well as any other identifying information or "known identities" mParticle has collected about the user, such as Customer ID and email address. mParticle also tracks user's IP address and the first and last time it has "[s]een" the user on websites or apps incorporating its SDK.[36]

75.   The profiles mParticle maintains about each specific user also contain a "User Attributes" section.[37] This section lists all "available user attributes" which are updated from new "inbound data streams" including data sent via its SDK and other tracking technology.[38] These attributes can include the user's age, full name, gender, phone number,

---

[34] *What is MPID?*, MPARTICLE, https://support.mparticle.com/hc/en-us/articles/12812598876173-What-is-a-MPID (Apr. 22, 2025).

[35] *Id.*

[36] *Customer Profiles Overview*, MPARTICLE, https://docs.mparticle.com/guides/customer-360/profiles/overview/ (last visited Apr. 22, 2025).

[37] *User Profiles*, MPARTICLE, https://docs.mparticle.com/guides/customer-360/profiles/user-profiles/ (last visited Apr. 22, 2025).

[38] *Id.*; *Start Capturing Data*, MPARTICLE, https://docs.mparticle.com/guides/getting-started/start-capturing-data/ (last visited Apr. 22, 2025); *Feeds*, MPARTICLE, https://docs.mparticle.com/guides/feeds/ (Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

address, city, state, zip code, and country, which are used for deterministic identity mapping.

FIGURE 2
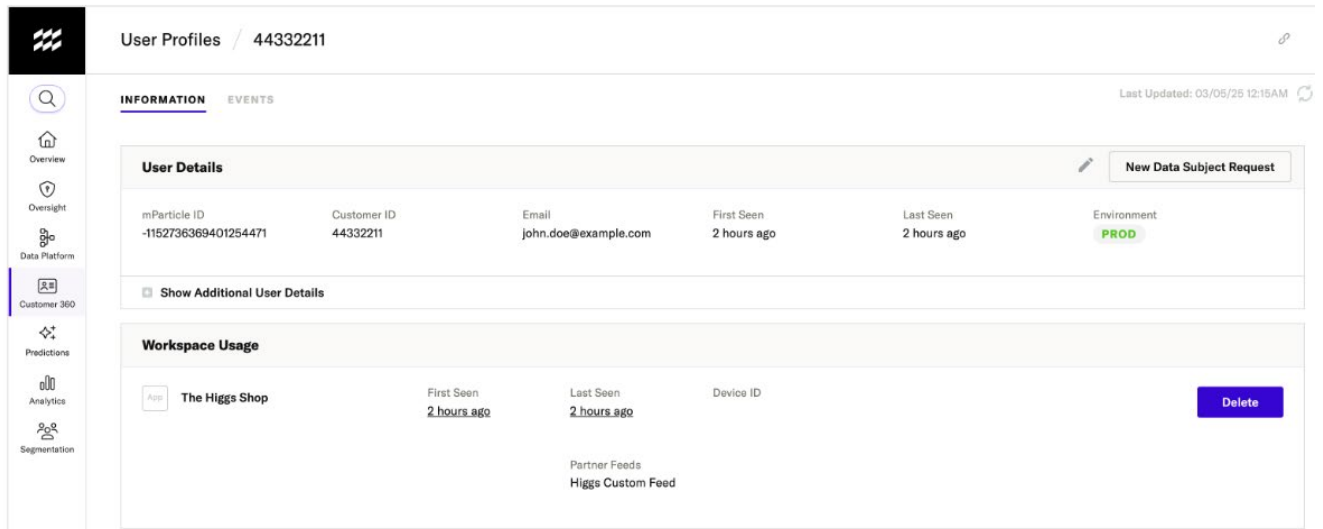
76.   The profile also contains event data, which are tied to specific actions the user has taken on the website or app. This includes, for example, the video titles and video IDs for the videos that Plaintiff Hayward accessed and viewed on the Peacock App. mParticle also tracks in each user's profile the audiences the user is a part of and whether they are currently included in any advertising campaigns.

77.   As long as the client keeps mParticle's SDK incorporated, mParticle "continues to collect data about the user's behavior" and storing in the user's profile.[39] mParticle's tracking technology automatically updates new identifying information as "User identity change" and "User attribution change."[40]

78.   mParticle does not obtain user consent before it collects their identifying information or before it stiches the information together into a comprehensive user profile. Users cannot prevent mParticle's tracking technology and IDSync service from tracking them by declining cookies, using private browsing mode, or Apple's "Do Not Track"

---

[39] *Identify Users*, mParticle, https://docs.mparticle.com/guides/idsync/identify-users/ (last visited Apr. 22, 2025).

[40] *Event Tracking*, MPARTICLE, https://docs.mparticle.com/developers/client-sdks/android/event-tracking/ (last visited Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

feature. In fact, most—if not all—users have no idea that mParticle is tracking, storing, compiling, and selling their private data.

79. This makes mParticle's tracking software even stronger than identifiers that previously existed, at the expense of the individual's right to privacy.

MPARTICLE'S DATA ENRICHMENT & MACHINE LEARNING

80. Even though it is a significant and highly offensive privacy intrusion, mParticle's improper conduct does not end at unique, individual-level tracking across all of a user's internet-connected devices.

81. Instead, mParticle also uses the data it receives to power its machine learning models. These models "analyze thousands of behavioral signals" to figure out which "users are statistically most likely to convert" based on their client's conversion goals.[41] A "conversion" is advertising-speak for a customer buying a product or paying money for the advertised service.

82. The results from these machine learning models are provided to mParticle's clients as "Predictive Attributes" that are stored in the user profile.[42] These predicative attributes are updated "automatically based on real-time customer behavior."[43] The model "continuously recalculates" the attributes based on the user's activity.[44]

83. For example, one of mParticle predictive attributes is "how likely [a user is] to take a specific action" that matter to its client's business. mParticle can "predict[]" and "anticipate"[45] the user's likelihood to take this action because of its machine learning processes, run on thousands of data fields, and its existing information about the user.

84. mParticle's machine learning—and detailed user profiles—are also used to create "predictive audiences"—groups of users whose mParticle's machine learning

---

[41] *What About Predictive Attributes*, MPARTICLE, https://docs.mparticle.com/guides/customer-360/predictive-attributes/overview/ (last visited Apr. 22, 2025).
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Predictive Audiences Overview*, MPARTICLE, https://docs.mparticle.com/guides/segmentation/predictive-audiences/overview/ (last visited Apr. 22, 2025).

CLASS ACTION COMPLAINT – CASE NO. _____

capabilities predict are all likely to take the same or similar action.[46]

85.   Separately, one of mParticle's primary selling points is that it also "[e]nrich[es]" raw user data, making it more specific and actionable.[47] As explained by mParticle, it receives data in "batches" through its SDK, API, or other means. During data processing, mParticle compares the data batch to the "matching user profile and adds additional information" about the user before it is sent along to third parties through integrations (described below).[48]

FIGURE 3
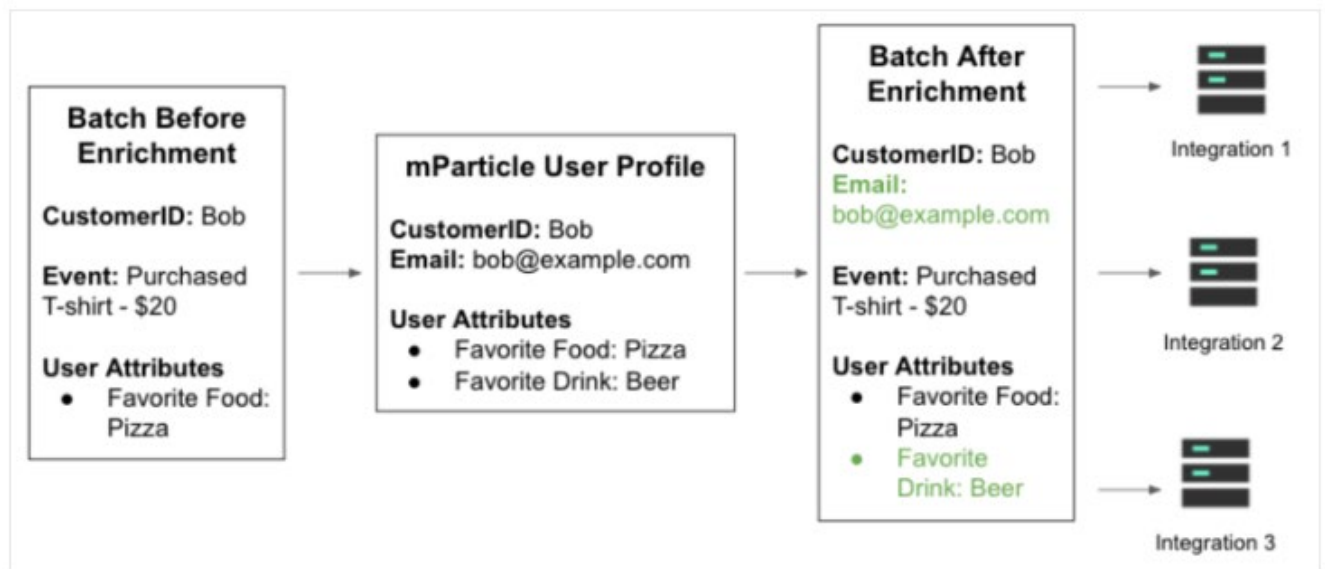
86.   As shown in Figure 3, mParticle adds data fields to the data "batch." In this example, even though the data batch previously only contained Bob's favorite food (pizza), mParticle was able to add from Bob's user profile the fact that Bob's favorite drink is beer. mParticle also appended Bob's email to the data batch, which it pulled from the mParticle User Profile.

87.   mParticle advertises that this "enrichment" process is particularly useful to "ensure[]" that "downstream tools" (i.e., advertising companies) "receive complete and

---

[46] *Predictive Audiences Overview*, MPARTICLE, https://docs.mparticle.com/guides/segmentation/predictive-audiences/overview/ (last visited Apr. 22, 2025).

[47] *Customer Profiles Overview*, MPARTICLE, https://docs.mparticle.com/guides/customer-360/profiles/overview/ (last visited Apr. 22, 2025).

[48] *Id.*

CLASS ACTION COMPLAINT – CASE NO. _____

accurate information about [the] users."[49] These downstream tools and integrations are described further in the next section.

88. Thus, what mParticle is really "enriching" is itself, by cashing in on its hidden and unauthorized collection of millions of internet and app users' private data

MPARTICLE'S INTEGRATION WITH ADVERTISING PLATFORMS

89. The mParticle ID, and accompanying user profiles, are especially problematic because they can be and are in fact shared with advertising companies and other identity providers—such as Google, Meta, and Adobe—to enable consistent personalization and targeting across platforms.

90. When an "integration" is enabled, mParticle "forwards" its user profiles and the accompanying data directly to these advertisers and identity providers. This data can be forwarded server-side (where it cannot be observed by even data scientists) or through the user's browser.[50]

91. For example, as shown in Figure 4, one integration mParticle offers is with Facebook. mParticle can forward user's emails, Facebook IDs, IDFA, Google Advertising IDs, and phone numbers directly to Facebook, as well as user "attributes" and event data, as described in the previous section.[51]

---

[49] *Id.*

[50] *Audience*, MPARTICLE, https://docs.mparticle.com/integrations/facebook/event/ (last visited Apr. 22, 2025).

[51] *Id.*

CLASS ACTION COMPLAINT – CASE NO. _____

FIGURE 4[52]

CLASS ACTION COMPLAINT – CASE NO. _____

92.   mParticle recommends its clients enable forwarding email address and Facebook ID "whenever they are available," because they "result in higher match rates with Facebook users."[53]

93.   Once integrated with Facebook, mParticle customers can use these down-stream versions of the data to create "value-based lookalike audiences" in Facebook to target users who share similar characteristics and behaviors with the customer's existing "high-value customers."[54] Customers can also combine mParticle's user profiles with Facebook's advanced matching features, thus enabling the user to be targeted at an even more specific level than they were originally.

94.   Similarly, mParticle allows integration with Google Ads. mParticle can forward its user profile data to Google Ads, thus enabling Google to identify individuals based on email, phone numbers, or device IDs. It can also send physical address information to Google Ads for "advanced matching."[55] Like with Facebook, mParticle also transmits event data, including "custom events," to Google.[56] Once Google Ads receives the identity profiles and event data, it would allow Google's advertising client to create "Customer Match list" for hyper-specific targeted advertising.[57]

95.   This data-forwarding process compounds Defendant's violations of Plaintiff and Class Members' privacy, as mParticle readily hands over the data it should have never had to some of the largest and most privacy-invasive companies in the world.

PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

---

[52] *Audience*, MPARTICLE, https://docs.mparticle.com/integrations/facebook/audience/ (last visited Apr. 22, 2025).

[53] *Id.*

[54] Karola Karlson, *NEW! Facebook Value-based Lookalike Audiences – The Complete Guide*, ADESPRESSO BY HOOTSUITE (June 26, 2017) https://adespresso.com/blog/facebook-value-based-lookalike-audiences/.

[55] *Audience*, MPARTICLE, https://docs.mparticle.com/integrations/google-ads/audience/ (last visited Apr. 22, 2025).

[56] *Id*.

[57] *Id*.

CLASS ACTION COMPLAINT – CASE NO. _____

96. Internet users do not expect to be tracked across every single one of their internet-connected devices, including their web browser, apps, TVs, and more, without any disclosure of what is taking place or ability to prevent it.

97. Indeed, the advent of privacy-preserving mechanisms like Apple's "Do Not Track" feature, which prevents companies from collecting IDFA/ADID from individuals who opt-out, have confirmed this expectation.

98. One study by Flurry Analytics in 2021 shows that 88% of iOS users worldwide have availed themselves of this feature, indicating an intent to prevent apps from tracking them on their mobile devices.

99. Users do not know—and did not expect—that mParticle would circumvent these protections by creating a new identifier and user profiles that are even *better* than IDFA/ADID at uniquely identifying them at the individual level.

100. mParticle itself does not provide any disclosures at the point of interception for Plaintiff and Class Members to understand which websites or online services use their mParticle ID. As a result, Plaintiff and Class Members have no way of uncovering which services do or do not contain mParticle's tracking technology.

101. As described above, there also is no way for Plaintiff or Class Members to opt out of mParticle's tracking at the time of the interception or to avoid mParticle capturing, storing, and tracking their use of apps and websites, or its sharing of that data with undisclosed third parties.

102. Plaintiff and Class Members reasonably expected that their online activity would not be tracked by an unknown company, let alone that their data—including personally identifiable information such as email addresses and phone numbers—would be used to target them across online services for profit.

103. mParticle did not have consent to perform this type of omni-present cross-device tracking using Plaintiff's and Class Members' email addresses and phone numbers.

CLASS ACTION COMPLAINT – CASE NO. _____

104.   That mParticle did not have consent is clear from its own CCPA disclosures. According to mParticle, they received only **_one_** request under the CCPA's right to know laws over a **_four-year period_**.

FIGURE 5[58]

CCPA Requests received by mParticle

	To Know	To Delete	Opt Out	Average Time to Respond
2020	1	0	0	7 days
2021	0	0	0	0 days
2022	0	0	0	0 days
2023	0	0	0	0 days

105.   These statistics confirm that almost no consumers knew of mParticle and certainly did not consent to its omnipresent data collection and user profiling.

TOLLING & CONCEALMENT

106.   The earliest Plaintiff and Class Members could have discovered mParticle's conduct was shortly before the filing of this Complaint. Plaintiff became aware of mParticle's conduct through communications with counsel that are protected from disclosure.

107.   Plaintiff and Class Members, despite their due diligence, could not have discovered mParticle's conduct by virtue of how the technology works and its lack of disclosures.

108.   mParticle's interception of personally identifiable information and assignment of an mParticle ID happens inconspicuously in the background. This process is undetectable to an ordinary person, highly technical, and prevented Plaintiff and any Class Member from uncovering it.

---

[58] *Privacy Policy*, MPARTICLE, (Apr. 18, 2024) https://www.mparticle.com/privacypolicy/.

CLASS ACTION COMPLAINT – CASE NO. _____

109.   mParticle had exclusive knowledge that it was tracking Plaintiff and Class Members across the internet and compiling their directly identifiable information and other data. Similarly, mParticle had exclusive knowledge that it was using this information to propagate comprehensive user profiles to train its machine learning models and to sell to third parties.

110.   mParticle's fraudulent conduct prevented Plaintiff and Class Members from discovering its conduct. mParticle maintained a privacy policy that lacked adequate disclosures for Plaintiff and Class Members to uncover mParticle ever intercepted, had, or used their data. mParticle publicly held out its identifiers and technology as privacy-preserving mechanisms, even though they were not.

111.   mParticle was under a duty to disclose the nature and significance of its data interception and use practices—especially in light of its public statements—but did not do so. mParticle is therefore estopped from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

112.   Plaintiff brings this action under Fed. R. Civ. P. 23 individually and on behalf of the following Classes:

> **Identifier Class:** All natural persons in the United States who were assigned an mParticle ID or had their personally identifiable information intercepted by, or shared with, mParticle.

> **Communications Class**: All natural persons in the United States who had their communications with third parties intercepted by, shared with, or used by mParticle without their consent.

113.   The Classes exclude: (1) any judge presiding over this action or their immediate families; (2) mParticle, its subsidiaries, affiliates, parents, successors, predecessors, and any other entity in which mParticle has a controlling interest; (3) mParticle's current and former employees, officers, and directors; and (4) Plaintiff's and mParticle's counsel.

CLASS ACTION COMPLAINT – CASE NO. _____

114.   ***Numerosity.*** While the precise size of the Classes are currently unknown to Plaintiff, each of the Classes consists of well over a million individuals and members of each of the Classes can be identified through mParticle's records.

115.   ***Predominant Common Questions.*** The Classes' claims present several common questions of law and fact that predominant over questions (if any) that affect individual class members. This includes:

    a. Whether mParticle violated Plaintiff's and the Classes' privacy rights;

    b. Whether mParticle engaged in unfair and deceptive conduct;

    c. Whether mParticle's acts and practices violate the California Invasion of Privacy Act;

    d. Whether Plaintiff and Class Members are entitled to damages and/or equitable relief, including injunctive relief, restitution, and disgorgement; and

    e. Whether mParticle was unjustly enriched.

116.   ***Typicality***. Plaintiff's claims are typical of all Class Members because they arise from the same conduct and are based on the same legal theories.

117.   ***Adequate Representation***. Plaintiff will (and has) fairly and adequately represented the Classes and protected the interest of all Class Members. Plaintiff has retained competent counsel with significant experience in class action and data privacy litigation. Plaintiff and counsel have no interest that conflicts with the interests of the Classes and is not subject to any unique defenses. Plaintiff and their counsel will vigorously prosecute this action to advance the interest of the Classes and have the resources necessary to do so.

118.   ***Substantial Benefits***. A class action is superior to all other possible methods to fairly and efficiently adjudicate this case and controversy, and joinder of all Class Members is impracticable. Proceeding as a class case has significant advantages to individual litigation, including: (1) comprehensive oversight by a single court, which avoids inconsistent outcomes; and (2) saving time and expense by litigating the same claims arising from the same conduct all in one action.

119.   Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal developments following additional investigation or discovery.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

120.   California law applies to every Class Member's claims. mParticle conducts substantial business in California, including the activities giving rise to Plaintiff's and Class Members' claims. California has a substantial, overriding interest in regulating the conduct of mParticle under its laws. mParticle's decision to maintain an office in California and avail itself of California's laws makes the application of California law to its conduct alleged herein constitutionally permissible.

121.   Under California's choice of law rules, the application of California law is appropriate because California has significant contacts to the claims and Parties in this action, California has a greater interest in applying its laws, given mParticle's presence in the State and the location of the conduct at issue, over any other state.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Violation of Common Law Invasion of Privacy (Intrusion Upon Seclusion)
On Behalf of the Plaintiff and Classes

122.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

123.   Intrusion upon seclusion requires pleading: (1) that the defendant intruded on a place, conversation, or matter in which plaintiff has a reasonable expectation of privacy; and (2) that the intrusion would be highly offensive to a reasonable person.

124.   mParticle's collection, interception, and use of Plaintiff and Class Members' directly identifiable information, unique identifiers, and private communications constitutes an intentional intrusion.

125.   mParticle's interception and use of Plaintiff and Class Members private online communications, associated with their mParticle ID and user profile, is likewise an intentional intrusion upon Plaintiff and Class Members' solitude.

CLASS ACTION COMPLAINT – CASE NO. _____

126.   Plaintiff and Class Members reasonably expected their personally identifiable information, alongside their online activity, would not be intercepted or used by an unknown third-party. Email addresses and phone numbers are particularly private because they are directly identifiable, permanent identifiers. Plaintiff and Class Members reasonable expected this information would remain private and confidential and would not be intercepted or used by third parties without their consent.

127.   This expectation is particularly heightened given that there were no disclosures of mParticle's involvement in intercepting, processing, and using their personally identifiable information and online communications.

128.   Plaintiff and Class Members did not consent to, authorize, or understand mParticle's interception or use of their private data.

129.   mParticle's conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they use the internet, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

130.   mParticle's conduct is particularly offensive in light of the secretive nature in which it takes place. Plaintiff and Class Members had no way of knowing mParticle collected their personally identifiable information and other online communications, and mParticle did so from thousands of websites, if not more.

131.   mParticle's conduct caused Plaintiff and Class Members harm and injury, including a violation of their privacy interests.

132.   Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by mParticle as a result of its intrusion upon seclusion.

133.   Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's and Class Members' rights. Thus, Plaintiff and Class Members are entitled to punitive and exemplary damages.

CLASS ACTION COMPLAINT – CASE NO. _____

134.   Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

SECOND CAUSE OF ACTION

**Violation of Article I, Section 1 of the California Constitution (Invasion of Privacy)
On Behalf of the Plaintiff and Classes**

135.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

136.   Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." California Constitution, Article I, Section 1.

137.   To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

138.   The right to privacy in California's constitution creates a right of action against private and government entities.

139.   Plaintiff and Class Members have and continue to have a reasonable expectation of privacy in their personal information, identities, and private data, pursuant to Article I, Section I of the California Constitution. The manner in which mParticle intercepted this information defeated established privacy-mechanisms and social norms.

140.   This conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person. Reasonable individuals do not expect that there is an entity intercepting and monitoring all of their online activity, let alone using it to compile online profiles for profit.

141.   mParticle's conduct violated the privacy of hundreds of millions of Class Members, including Plaintiff. mParticle did not have consent to intercept this information, let alone use it.

CLASS ACTION COMPLAINT – CASE NO. _____

142.   Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by mParticle as a result of its intrusion upon seclusion.

143.   Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's and Class Members' rights, Plaintiff and Class members are entitled to punitive and exemplary damages.

144.   Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

THIRD CAUSE OF ACTION
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code § 631
On Behalf of the Plaintiff and Classes

145.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

146.   CIPA § 631 prohibits any person who uses a "machine, instrument, contrivance" or in "any other manner": (1) intentionally taps or makes an unauthorized connection with "any telegraph or telephone wire, line, cable, or instrument"; (2) willfully and without consent of "all parties to the communication" or in "any unauthorized manner" reads or "attempts to read" or "learns the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within" California; (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way" information so obtained; or (4) from aiding, agreeing, employing, or conspiring with "any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

147.   mParticle is a person under CIPA § 631.

148.   mParticle designed, created, conspired, and effectuated the interception and use of Plaintiff's and Class Members' personally identifiable information and private communications in California because (1) Plaintiff is based in California, where mParticle

CLASS ACTION COMPLAINT – CASE NO. _____

intercepted his personally identifiable information and private communications; (2) it developed profiles on California citizens, including Plaintiff; and (3) it partners and cooperates with advertising companies in California—like Google, LLC—to use these user profiles, including those maintained on California citizens.

149.   mParticle's technology (e.g., the IDSync system, mParticle ID, mParticle SDK etc.), and Plaintiff's and Class Members' computers, mobile devices, and connected TVs, are a "machine, instrument, contrivance, or . . . other manner" under CIPA § 631.

150.   At all relevant times, mParticle used its technology to make unauthorized connections with the lines of communication and instruments used by Plaintiff and Class Members to access online services without the consent of all parties to those communications.

151.   mParticle willfully, and without consent, read or attempted to read, or learn the contents and meaning of, Plaintiff's and Class Members' private communications with online services while those communications were in transmit or passing over a wire, line, or cable, or were being sent or received within California through the IDSync framework and its tracking technology, as described herein. This interception happens prior to or at the same time they would be received by the intended recipient.

152.   mParticle used, and attempted to use, these identifiable, private communications for its own benefit, including for data enrichment and to facilitate targeted advertising through its integrations—all for profit.

153.   mParticle also aided, agreed with, employed, and conspired with other advertising and identity platforms to intercept and use this data for profit.

154.   The interception and use of Plaintiff's and Class Members' communications was without authorization or consent from Plaintiff and Class Members.

155.   Plaintiff and Class Members have been harmed as a result of mParticle's conduct. Their private data has been intercepted, viewed, and used for targeted advertising and has not been destroyed. Plaintiff and Class Members face an imminent threat of

CLASS ACTION COMPLAINT – CASE NO. _____

continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

156.   Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

<div align="center">

FOURTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632
On Behalf of the Plaintiff and Classes

</div>

157.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

158.   Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

159.   Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

160.   Plaintiff's and Class Members' communications to online services are confidential communications for purposes of § 632, because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data.

161.   Plaintiff and Class Members expected their communications would not be shared with mParticle, as there were no disclosures that mParticle would secretly eavesdrop upon or record their information and communications.

162.   mParticle's IDSync framework and other tracking technology are electronic amplifying or recording devices for purposes of § 632.

163.   By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential and identifiable communications to online services through this

<div align="center">

31

CLASS ACTION COMPLAINT – CASE NO. _____

</div>

technology, mParticle eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

164. At no time did Plaintiff or Class Members consent to mParticle's conduct, nor could they reasonably expect that their communications with online services would be overheard and recorded by mParticle.

165. mParticle utilizes these private communications for their own benefit, including to enrich and enhance the data, create comprehensive user profiles, and facilitate targeted advertising through its integration offerings—all for profit.

166. Plaintiff and Class Members have been harmed as a result of mParticle's conduct. Their private data has been intercepted, viewed, and used, and has not been destroyed. Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

167. Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 638.50 & 638.51
On Behalf of the Plaintiff and Classes

168. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

169. CIPA § 638.50(b) defines a "pen register" as a "device or process" that "records or decodes dialing, routing, addressing, or signaling information" that is "transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

170. Separately, CIPA § 638.50(c) defines a "[t]rap and trace device" as a "device or process that captures the incoming electronic or other impulses that identify the

CLASS ACTION COMPLAINT – CASE NO. _____

originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication."

171.   CIPA § 638.51 prohibits a person from installing either a pen register or trap and trace device without a court order.

172.   mParticle is a person under CIPA § 638.51.

173.   mParticle implemented and installed the IDSync framework and other tracking technology—which are pen registers and/or trap and trace devices—on Plaintiff's and Class Members' devices and browsers.

174.   These processes captured "routing, addressing, or signaling information" because they intercept: (1) users' directly identifiable information, including email addresses or phone numbers; (2) other unique user identifiers; and (3) information indicating the recipient of the communication.

175.   mParticle was not authorized by any court order to use a pen register or trap and trace device to record or capture Plaintiff's and Class Members' routing, addressing, or signaling information.

176.   Plaintiff and Class Members did not consent to mParticle's installation of a pen register or trap and trace device on their devices and browsers.

177.   Plaintiff and Class Members have been harmed as a result of mParticle's conduct. mParticle did not have authorization to use pen registers and/or trap and trace devices to surveille and identify Plaintiff and Class Members or other routing, addressing, and signaling information revealing who the intended recipients of their communications were.

178.   Plaintiff and Class Members face an imminent threat of continued injury, as this data continues to be stored and used, such that Plaintiff and Class Members have no adequate remedy at law.

179.   Plaintiff and Class Members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the

1 amount of damages sustained by Plaintiff and the Classes in an amount to be proven at

2 trial, as well as injunctive or other equitable relief.

SIXTH CAUSE OF ACTION
**Violation of the Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502 ("CDAFA")
On Behalf of the Plaintiff and Classes**

6   180.   Plaintiff re-alleges and incorporates the preceding allegations of this

7 Complaint with the same force and effect as if fully restated herein.

8   181.   The California Legislature enacted the CDAFA to "expand the degree of

9 protection afforded . . . from tampering, interference, damage, and unauthorized access to

10 [(including the extraction of data from)] lawfully created computer data and computer

11 systems," finding and declaring that "the proliferation of computer technology has resulted

12 in a concomitant proliferation of . . . forms of unauthorized access to computers, computer

13 systems, and computer data," and that "protection of the integrity of all types and forms of

14 lawfully created computers, computer systems, and computer data is vital to the protection

15 of the privacy of individuals . . ." Cal. Penal Code § 502(a).

16   182.   Plaintiff's and Class Members' devices on which mParticle's tracking

17 technology is installed, including their computers, smart phones, and tablets, constitute

18 "Computer system[s]" within the meaning of the CDAFA. *Id.* § 502(b)(5).

19   183.   The data that mParticle accessed and collected from Plaintiff's and Class

20 Members' devices constitute "Data" within the meaning of the CDAFA. *Id.* § 502(b)(8).

21   184.   Defendant mParticle violated § 502(c)(1) of the CDAFA by knowingly

22 accessing and using without permission Plaintiff's and Class Members' devices in order to

23 wrongfully obtain and use their personal data, in violation of users' reasonable expectations

24 of privacy in their devices and data.

25   185.   Defendant mParticle violated § 502(c)(2) of the CDAFA by knowingly and

26 without permission taking, copying, and making use of Plaintiff's and the Class Members'

27 personally identifiable information from their devices.

28

CLASS ACTION COMPLAINT – CASE NO. _____

186.   Defendant mParticle's tracking technology incorporated on Plaintiff's and the Class Members' devices constitute "computer services" within the meaning of the CDAFA. Defendant mParticle violated § 502(c)(3) by knowingly and without permission using those computer services, and/or causing them to be used. Defendant mParticle violated § 502(c)(7) by knowingly and without permission accessing those devices, and/or causing them to be accessed.

187.   Defendant mParticle violated §§ 502(c)(6) and (c)(13) of the CDAFA by knowingly, and without permission from Plaintiff and the Class Members, providing and/or assisting in providing advertisers and ads publishers the ability to access Plaintiff's and the Class Members' personal data via its tracking technology.

188.   Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Defendants mParticle violated § 502(c)(8) by knowingly and without permission introducing a computer contaminant via its Tracking Technology incorporated on Plaintiff's and the Class Members' devices, which intercepted their personal data. As described *supra*, the tracking technology is deeply hidden; Plaintiff and Class Members had no way to remove it or opt out of its functionality.

189.   Plaintiff and Class Members suffered damage and loss as a result of mParticle's conduct. mParticle's practices have deprived Plaintiff and the Class Members of control over their valuable property (namely, their sensitive personal data), the ability to receive compensation for that data, and the ability to withhold their data for sale.

190.   Plaintiff and the Class Members seek compensatory damages in accordance with CDAFA § 502(e)(1), in an amount to be proven at trial, and injunctive or other equitable relief.

191.   Plaintiff and Class Members have also suffered irreparable and incalculable harm and injuries from mParticle's violations. The harm will continue unless mParticle is

enjoined from further violations of this section. Plaintiff and Class Members have no adequate remedy at law.

192.   Plaintiff and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because mParticle's violations were willful and, upon information and belief, mParticle is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294. Plaintiff and the Class Members are also entitled to recover their reasonable attorneys' fees under § 502(e)(2).

<div align="center">

SEVENTH CAUSE OF ACTION
Unjust Enrichment
On Behalf of the Plaintiff and Classes

</div>

193.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

194.   mParticle receives benefits from Plaintiff and Class Members in the form of their personally identifiable information and private online communications. mParticle acquired this information without Plaintiff's and Class Members' authorization and without providing corresponding compensation.

195.   mParticle acquired and used this private data for its own benefit, including tangible economic benefits from companies that used mParticle for data enrichment, user identification, and to facilitate targeted advertisements.

196.   Had Plaintiff and Class Members known of mParticle's misconduct, they would not have agreed mParticle could acquire and use their private data.

197.   mParticle unjustly retained these benefits at the expense of Plaintiff and Class Members. Plaintiff and Class Members were harmed by this conduct and were not provided any commensurate compensation.

198.   The benefits mParticle received and derived from Plaintiff and Class Members' private data rightly belong to Plaintiff and Class Members. It is inequitable under unjust enrichment principles for mParticle to retain the profits and other intangible benefits they derived through its wrongful conduct.

CLASS ACTION COMPLAINT – CASE NO. _____

199.   mParticle should be compelled to disgorge these profits and other inequitable proceeds in a common fund for the benefit of Plaintiff and Class Members.

EIGHTH CAUSE OF ACTION
Injunctive Relief
On Behalf of the Plaintiff and Classes

200.   Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

201.   mParticle's conduct has and continues to cause harm to Plaintiff and Class Members' privacy and autonomy, as it continues to maintain comprehensive user profiles, as well as the private contents of their communications, on its own systems. mParticle routinely shares this information with other third parties to facilitate targeted advertising.

202.   Accordingly, Plaintiff and Class Members seek injunctive relief, including an order permanently restraining mParticle from continuing to use and store this information without consent and/or a court order, and requiring mParticle to delete this information from its systems.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the putative Class requests the Court enter an Order:

    a. Certifying the Classes and appointing Plaintiff as Class Representative;

    b. Finding mParticle's conduct unlawful;

    c. Awarding injunctive and other equitable relief as is just and proper;

    d. Awarding Plaintiff and the Classes statutory, actual, compensatory, punitive, nominal, and other damages, as well as restitution and/or disgorgement of unjust and unlawful profits;

    e. Awarding pre-judgment and post-judgment interest;

    f. Awarding reasonable attorneys' fees, costs, and expenses; and

    g. Granting any other relied as the Court sees just and proper.

Dated: April 23, 2025

/s/ Heather Lopez
Heather Lopez (SBN 354022)
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: hlopez@milberg.com

Christian Levis (*pro hac vice* forthcoming)
Amanda Fiorilla (*pro hac vice* forthcoming)
Rachel Kesten (*pro hac vice* forthcoming)
Yuanchen Lu (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com
ylu@lowey.com

CLASS ACTION COMPLAINT – CASE NO. _____